УДК 681.3.06

А.В. ЛЄНШИН, П.В. БУСЛОВ

Харківський національний університет радіоелектроніки, Україна

МЕТОД ФОРМУВАННЯ ФУНКЦІОНАЛЬНИХ ПРОФІЛІВ ЗАХИЩЕНОСТІ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Проведено аналіз вимог нормативних документів в частині формування профілів захищеності. Визначені недоліки існуючого підходу до формування профілю захищеності. Сформульовані вимоги до методу формування профілів захищеності, надано його опис. Показано, що розроблений метод відповідає вимогам із: часової складності, стандартизованості підходу (повторюваність і порівнюваність результатів), несуперечності нормативним документам, зрозумілості проміжних результатів та їх впливів на остаточний вибір, а також можливості самоперевірки особи, що використовує метод.

Ключові слова: *профіль захищеності, захист інформації, критерії оцінки захищеності від несанкціонованого доступу, комплексна система захисту інформації.*

Вступ

Як визначено у [1, 2] захист інформації з обмеженим доступом або інформації, захист якої гарантується державою, має здійснюватися за рахунок створення комплексної системи захисту інформації (КСЗІ) із врахуванням вимог нормативно-правових документів у сфері криптографічного (КЗІ) та технічного захисту інформації (ТЗІ). Якщо інформація зазначених видів не обробляється, вимоги щодо КЗІ та ТЗІ носять рекомендаційний характер.

Згідно з законодавством України [1] під ТЗІ розуміють діяльність, спрямовану на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації. Базовим документом, що регламентує зміст та порядок робіт із забезпечення захисту інформації є технічне завдання на КСЗІ. Вимоги до КСЗІ мають формулюватися [3] в частинах: захисту від несанкціонованого доступу (НСД) та захисту від витоку інформації технічними каналами. Вимоги щодо захисту від НСД викладаються у вигляді опису послуг політики безпеки, яку має реалізовувати комплекс засобів захисту (КЗЗ) та функціонального профілю захищеності (ФПЗ).

Ця робота присвячена розробці методу, який дозволить обирати послуги безпеки (та визначати їх рівні), що мають бути включені до ФПЗ, із врахуванням вимог політики безпеки та множини загроз безпеці інформації для комп'ютерної системи (КС). До методу, що розробляються, висуваються підвищені вимоги із: часової складності, стандартизованості підходу (повторюваність та порівнюваність результатів), несуперечності нормативним документам, зрозумілості проміжних результатів та їх впливів на остаточний вибір, а також можливості самоперевірки особи, що його використовує.

1. Аналіз стандартного підходу до формування ФПЗ

У 1999 році ТОВ "Інститут комп'ютерних технологій" було розроблено НД ТЗІ 2.5-004-99 [4] який визначає критерії оцінки захищеності комп'ютерних систем від НСД та НД ТЗІ 2.5-005-99 [5], що надає нормативно-методологічну базу для вибору та реалізації вимог із захисту інформації в автоматизованій системі (АС). Одночасне прийняття зазначених документів [4, 5] не було випадковим, оскільки для фахівців, що формують вимоги до КС дуже актуальною є задача визначення набору послуг безпеки, що дійсно необхідні для середовища КС, а також рівня з яким вони мають забезпечувати захист від існуючих загроз. Єдиним документом у якому надано опис послуг безпеки є НД ТЗІ 2.5-004-99 (додаток А), проте він розроблявся з метою надання порівняльної шкали для оцінки надійності механізмів захисту та орієнтирів для розробки КС із функціями захисту інформації. Ось чому питання вибору послуг безпеки, що потрібні для конкретної КС із урахування середовищ та моделі загроз осталося у НД ТЗІ 2.5-004-99 поза розглядом. У документі [5] визначено підхід до визначення ФПЗ шляхом вибору з множини стандартних ФПЗ. Зважаючи на те, що цей підхід є єдиним, що визначений у НД ТЗІ та для спрощення викладення матеріалів, далі у статті використовується термін "стандартний підхід". Стандартний підхід базується на таких припущеннях:

а) Усі АС можна віднести до одного з трьох класів за наступними ознаками: конфігурація апаратних засобів, їх фізичне розміщення, кількість категорій оброблюваної інформації, кількість користувачів і категорій користувачів.

б) У межах класу АС можна віднести до одного з підкласів, що визначені за критерієм необхідності забезпечення: конфіденційності, цілісності та доступності інформації. Таким чином кількість сполучень з трьох властивостей зумовлює наявність семи підкласів АС (таблиця 1).

в) Вимоги до безпеки АС різних класів суттєво відрізняються, що дозволяє сформувати для їх підкласів множини стандартних ФПЗ, що знаходяться у ієрархічній залежності (реалізація забезпечує наростаючу захищеність від загроз певного типу).

г) Для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної АС, необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків.

Визначено такі етапи застосування стандартного підходу для визначення ФПЗ для КС, що використовується у складі АС.

Е1) Визначення класу АС. Е2) Визначення яке сполучення вимог конфіденційності, цілісності, доступності висувається до АС. Е3) Визначення призначення АС та вибір підказки ("маски") яку треба використовувати у цьому випадку для вибору одного зі стандартних ФПЗ (використовуючи, довідковий додаток А з НД ТЗІ 2.5-005-99). Якщо призначення АС відрізняється від наведених у [5] необхідно власноруч обрати підмножину стандартних ФПЗ, відповідно до класу АС у якій експлуатується КС. Е4) Аналіз сутності вимог, відібраних стандартних ФПЗ. Е5) Вибір одного зі стандартних ФПЗ, що найбільш відповідає політиці безпеки. Е6) У випадку, коли жоден із стандартних ФПЗ не підходить повною мірою, необхідно змінити рівень послуги, що міститься у стандартному ФПЗ, або додати нову послугу. При цьому необхідно врахувати залежності між послугами, що визначені у НД ТЗІ 2.5-004-99.

Таблиця 1

Кількість стандартних ФПЗ, що визначені у НД ТЗІ 2.5-005-99

Клас АС	Кількість стандартних ФПЗ для підкласів АС							Загальна кількість стандартних ФПЗ
	К	Ц	Д	КЦ	КД	ЦД	КЦД	
АС-1	2	2	4	2	4	4	4	22
АС-2	6	5	4	6	4	4	5	34
АС-3	6	5	4	6	4	4	5	34

Визначимо переваги та недоліки, що притаманні стандартному підходу. Основними перевагами є відносна простота за рахунок: наявності готових шаблонів ФПЗ для КС, можливості звуження простору вибору за рахунок визначення призначення АС (автоматизації діяльності органів державної влади, автоматизації банківської діяльності, керування технологічними процесами, довідково-пошукові системи) до складу якої входять КС, врахування необхідних зв'язків між послугами, що входять до складу стандартних функціональних ФПЗ. До основних недоліків слід віднести: значна складність (особливо часова) детального аналізу послуг безпеки, що входять до складу стандартних ФПЗ, відсутність формалізованого (та зрозумілого користувачу) зв'язку між включеними до стандартного ФПЗ послугами безпеки (їх рівнями) та загрозами і ризиками для конкретної КС. Власне кажучи, недоліки стандартного методу є наслідком його основної переваги. Стандартний ФПЗ не може повністю відповідати вимогам довільної КС, якщо кількість стандартних ФПЗ не дорівнює загальній кількості можливих ФПЗ, а у випадку рівності цих величин це вже не стандартні ФПЗ, а "припустимі профілі". Звісно, що використання у стандартному підходу "припустимих профілів" призвело б до надвеликої складності їх належного аналізу. Кількість стандартних ФПЗ для окремих підкласів [5] визначені у табл. 1.

Проведений аналіз [4] показав, що послуги безпеки вважаються більш-менш незалежними, за небагатьма виключеннями: послуга НЦ (цілісність КЗЗ) перший рівень якої, тобто НЦ-1 є обов'язковим для реалізації усіх інших послуг безпеки, а також деякими іншими залежностями, основними з яких є необхідність у реалізації послуг НО (розподіл обов'язками) та НИ (ідентифікація та автентифікація). Як видно з припущення б) щодо стандартного методу така властивість інформації як "спостереженість" не використовується для розбиття АС на підкласи. У роботі [5] цей факт пояснюється тим, що послуги спостереженості є необхідною умовою для реалізації інших послуг, а з іншого боку завжди важлива для КС. Проте швидше за все, не внесення властивості "спостережність" як такої, що визначає підклас, зумовлено тим, що розробники намагалися зменшити обсяг роботи особи яка приймає рішення (ОПР) щодо вибору ФПЗ за рахунок зменшення кількості стандартних ФПЗ.

2. Вимоги до методу формування ФПЗ

Проведений у першому розділі аналіз та недоліки стандартного підходу дозволив сформулювати такі вимоги до методу, що розробляється:

– зручність застосування (В1);

– зрозумілість проміжних результатів та їх впливу на остаточний склад ФПЗ (В2);

– врахування вимог нормативних документів у сфері ТЗІ (В3);

– коректність переходів між різними етапи визначення складу ФПЗ (В4);

– можливість самоперевірки ОПР (В5);

– наявність формалізованого процесу вибору та можливість використання результатів для документування ходу вибору елементів ФПЗ (В6);

– можливість інтеграції з іншими етапами побудови КСЗІ (В7).

Під В1 розуміється, логічність та ненадлишковість викладення текстової частини та використання у методі допоміжного інструментарію (наприклад, опитувальних листів, таблиць, формул, рисунків), що дозволять ОПР зосередитися на виконанні безпосередньо вирішуваної задачі – виборі елементів ФПЗ, а не на вивченні особливостей методу.

Під В2 розуміється можливість ОПР відстежувати яким чином її вибір на певному кроці впливає на проміжні/остаточні результати. Реалізація цієї вимоги необхідна для більшого залучення та творчої реалізації потенціалу ОПР, та надання можливості пошуку причин невідповідності (якщо такі є) сформованого ФПЗ наперед визначеним цілям або вимогам більш високого рівня, а також надання можливості вдосконалення/уточнення сформованого ФПЗ.

Вимога В3 передбачає несуперечливість вимогам/підходам, що викладені у діючих нормативних документах, а також розвиток принципів, що були задекларовані в них.

Для задоволення В4 алгоритм, що має бути покладений у основу метода, має забезпечувати відсутність "тупикових" ситуацій, тобто випадків в яких виникає неоднозначність трактування результатів (проміжних/остаточних) методу.

Необхідність виконання вимоги В5 полягає у підвищенні якості результатів процесу формування ФПЗ, зокрема несуперечливості положенням НД ТЗІ, а також надання ОПР можливості проконтролювати правильність своїх дій.

Вимога В6 висувається з метою підвищення рівня гарантій стосовно процесу розробки ФПЗ та загальної зрілості процесів захисту інформації.

Під В7 необхідно розуміти можливість використання результатів методу для виконання інших робіт зі створення КСЗІ, а також врахування у методі результатів попередніх етапів (наприклад, вимоги політики безпеки та моделі загроз).

3. Опис методу формування ФПЗ

На думку авторів статті, замість використання стандартного підходу, ефективнішим (у плані часової ефективності, та адекватності розподілу ресурсів, що використовується для захисту від загроз за рахунок реалізації послуг безпеки) є підхід який би з самого початку дозволив би обирати послуги безпеки (та їх рівні) виходячи із моделі загроз для конкретної АС. Такий висновок підтверджується припущенням г), що викладено у описі стандартного підходу, а також наведеними вище міркуваннями. Підхід, що пропонується дозволяє розв'язувати означене завдання не лише для АС але і для будь-якої КС. Слід відмітити, що оскільки НД ТЗІ 2.5-004-99 походить від "Канадських критеріїв" під терміном "КС" розуміється представлена для оцінки сукупність програмно-апаратних засобів (наприклад, автоматизована система, ЕОМ, засіб антивірусного захисту) і є аналогом терміну "Target of evaluation" (TOE) з ISO/IEC 15408.

Ідея авторів щодо розробки методу базується на визначенні ФПЗ. ФПЗ [4] – упорядкований перелік рівнів функціональних послуг безпеки. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного. Рівні починаються з першого і зростають до n, де n – унікальне для кожного виду послуги.

Можна стверджувати, що: 1) кожний клас послуг забезпечує захист від певного класу (сукупності) загроз (наприклад, клас послуг, що забезпечують захист від загроз конфіденційності); 2) кожна послуга забезпечує захист від певної множині загрози, що може бути названа загальною загрозою (наприклад, що буде порушена цілісність даних, які передаються через незахищене середовище – ЦВ); 3) кожний рівень послуги може бути поставлений у відповідність деталізованій загрозі (наприклад, загроза НСД до захищеного об’єкту з боку неавторизованого користувача у випадку коли користувачам дозволено керувати потоками інформації від захищених об’єктів КС до інших користувачів відповідає рівню КД-3).

Наведені припущення, а також аналіз опису послуг безпеки [4] дозволяє стверджувати, що для визначення необхідності реалізації конкретної послуги не потрібно розглядати усі критерії, яким має задовольняти послуга безпеки певного рівня. Це випливає з того, що при детальному розгляді значна кількість критеріїв вказує на те, що має робити КЗЗ, щоб послуга була реалізована, а не для чого потрібна ця послуга. Спираючись на [3] зробимо припущення, що, на момент написання ТЗ на КСЗІ вже існує політика безпеки та визначена модель загроз. Якщо це припущення вірне для первинного вибору послуг безпеки

необхідно та достатньо: 1) сформувати каталог загальних загроз; 2) сформувати каталог деталізованих загроз.3) проаналізувати випадки, що можуть свідчити про наявність помилки у визначені складу ФПЗ та виділити ознаки їх появи. Зазначені дії можна виконати на основі даних, що містяться у НД ТЗІ 2.5-004-99.

При розробці методу було зроблено спробу представити необхідні дії ОПР у вигляді алгоритму. Проте на практиці це виявилось не зручним (вимога В1). Тому алгоритми з'ясування необхідності та рівня послуги безпеки були подані у табличному вигляді (табл. 2).

Таблиця 2

Приклад таблиці для визначення необхідності та рівня послуги довірча конфіденційність (КД)

№	Запитання	Відповіді		Результат		Перехід до	Група відповідей
		Група	Варіанти відповіді	Зміст	Тип *		
1	Чи повинні користувачі (не адміністратори) мати можливість керувати потоками інформації від захищених об'єктів КС до інших користувачів?	а)	Так. Ця можливість має бути надана користувачам (не адміністраторам) стосовно окремих захищених об'єкті	Максимальний рівень послуги: "КД-2"	П	п.2	а)
			Так. Ця можливість має бути надана користувачам (не адміністраторам) стосовно всіх захищених об'єктів.	Мінімальний рівень послуги: "КД-3"	П	п.2	б)
			Ні. Таку можливість має бути виключено.	Послуга "КД" не потрібна	О	наступної таблиці	–
2	Захист від якого рівня загроз має забезпечувати КСЗІ?	а)	НСД до захищеного об'єкту із застосуванням неавторизованого процесу	Рівень послуги: "КД-1"	О	наступної таблиці	–
			НСД до захищеного об'єкту з боку неавторизованого користувача	Рівень послуги: "КД-2"	О	наступної. таблиці	–
		б)	НСД до захищеного об'єкту з боку неавторизованого користувача	Рівень послуги: "КД-3"	О	наступної. таблиці	–
			НСД до захищеного об'єкту з боку неавторизованого/авторизованого користувача із застосуванням неавторизованого процесу та/або НСД до захищеного об'єкту з боку авторизованого користувача із застосуванням неавторизованого процесу	Рівень послуги: "КД-4"	О	наступної. таблиці	–

*Примітка: "О" – остаточний результат, "П"– проміжний результат

Для задоволення В5 у методі було розроблено таблицю ознак появи помилок з такими графами: ознака, сутність помилки, дії, які необхідно вжити для усунення. Основними типами помилок, що враховуються є: не включення до ФПЗ послуг, що пов'язані (наприклад, якщо включено ДВ-1 необхідна, щонайменше і послуга НО-1), включення послуги безпеки, що не потрібні для АС певного класу (наприклад, для АС-1 не потрібна послуга КВ), одночасне визначення послуг, що не можуть використовуватися спільно (наприклад, ЦА-1 та ЦД-1) тощо.

При проектуванні методу було закладено такий принцип: перехід між таблицями не вимагає від ОПР додержання строго визначеного порядку, а лише вказує на необхідність послуг, що пов'язані. По-перше такий підхід вимагає від ОПР більш детального розуміння змісту та необхідності вимог, а не сліпого виконання сталої послідовності дій. По-друге викриті помилки свідчать про недосконаліть політики безпеки на основі якої розробляється ТЗ на КСЗІ або нерозуміння послуги безпеки.

Отже, застосування методу є ітераційною процедурою: К1) Відповідь на питання щодо всіх послуг безпеки (усього 22 таблиці, див. приклад у таблиці 2). К2) Вивчення сформованого ФПЗ на предмет наявності ознак помилок. К3) Уточнення сформованого ФПЗ або існуючої політики безпеки.

Висновки

Стандартний підхід має недоліки, основними з яких є: 1) неможливість доведення відповідності (та необхідності) послуг безпеки, що включені до ФПЗ та реальних загроз для КС; 2) велика часова складність аналізу вимог, що включені до стандартних ФПЗ. У роботі розроблено метод формування ФПЗ,

що позбавлений зазначених недоліків і задовольняє вимогам: зручність застосування, зрозумілість проміжних результатів, врахування вимог НД ТЗІ, можливість самоперевірки. Основою розробленого методу є: вибір послуг безпеки на основі моделі загроз для КС, використання опитувальних таблиць та таблиць самоперевірки. Перспективними напрямками досліджень вважаємо: формуванні ФПЗ з врахуванням моделі порушника, введення коефіцієнтів близькості ФПЗ до стандартних, розробка каталогів загальних та деталізованих загроз.

Література

1. Захист інформації. Технічний захист інформації. Основні положення: ДСТУ 3396.0-96.– [Чинний від 1996-10-11]. – К.: Держспоживстандарт України, 1996. – 10 с. – Текст: укр. – (Національний стандарт України).

2. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [Текст]: Затверджено наказом №22 ДСТСЗІ СБ України від "28" квітня 1999р. /ТОВ «Інститут комп'ютерних технологій». – К: ДСТСЗІ СБ України, 1999. -21с.- (Нормативний документ системи технічного захисту інформації).

3. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі [Текст]: Затверджено наказом №22 ДСТСЗІ СБ України від "28" квітня 1999 р. /ТОВ «Інститут комп'ютерних технологій». -К: ДСТСЗІ СБ України, 1999. -16с.- (Нормативний документ системи технічного захисту інформації).

4. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу [Текст]: Затверджено наказом №22 ДСТСЗІ СБ України від "28" квітня 1999 р. /ТОВ «Інститут комп'ютерних технологій». - К: ДСТСЗІ СБ України, 1999. -59с.- (Нормативний документ системи технічного захисту інформації).

5. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Текст]: Затверджено наказом №22 ДСТСЗІ СБ України від " 28 " квітня 1999 р. /ТОВ «Інститут комп'ютерних технологій». - К: ДСТСЗІ СБ України, 1999. -22с.- (Нормативний документ системи технічного захисту інформації).

Надійшла до редакції 27.01.2010

Рецензент: д-р техн. наук, доцент. заступник головного конструктора ЗАТ "ІІТ" О.В. Потій, ЗАТ "ІІТ", Україна.

МЕТОД ФОРМИРОВАНИЯ ФУНКЦИОНАЛЬНЫХ ПРОФИЛЕЙ ЗАЩИЩЕННОСТИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

А.В. Леншин, П.В. Буслов

Проведен анализ требований нормативных документов в части формирования профилей защищенности. Определены недостатки существующего подхода к формированию профиля защищенности. Сформулированы требования к методу формирования профилей защищенности, дано его описание. Показано, что разработанный метод соответствует требованиям по: временной сложности, стандартизированности подхода (повторяемость и сравнимость результатов), непротиворечивости требованиям нормативных документов, понятности промежуточных результатов и их воздействий на окончательный выбор, а также возможности самопроверки лица, использующего метод.

Ключевые слова: профиль защищенности, защита информации, критерии оценки защищенности от несанкционированного доступа, комплексная система защиты информации.

METHOD FOR DESIGN OF THE FUNCTIONALITY PROFILES OF UNAUTHORIZED ACCESS PROTECTION

A.V. Lyenshyn, P.V. Buslov

The analysis of the normative documents requirements concerning protection profiles is conducted. Shortcomings of existing approach to designing of protection profiles are identified. The requirements to the method for design of the functionality protection profile from unauthorized access are formulated and it description is given. Shown that the developed method complies with the requirements of: the time complexity, standardize the approach (repeatability and comparability of results), non-contradictory requirements of the normative documents, understandability of interim results and their impact on the final choice, as well as the possibility of self-verification for a person who uses the method.

Keywords: protection profile, information security, evaluation criteria of unauthorized access protection, complex information protection system.

Лєншин Анатолій Валерійович – канд. техн. наук, доц. кафедри безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, Харків, Україна, e-mail: l_a_v2002@mail.ru.

Буслов Павло Володимирович – магістрант кафедри безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, Харків, Україна, e-mail: buslov87@mail.ru.